

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
<small>Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.</small>				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 17 December 1998		3. REPORT TYPE AND DATES COVERED Monograph
4. TITLE AND SUBTITLE The Nonlethal Information Operations Targeting Process: DUTIES, RESPONSIBILITIES AND PROCEDURES				5. FUNDING NUMBERS
6. AUTHOR(S) Erin J. Gallogly-Staver				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) School of Advanced Military Studies Command and General Staff College Fort Leavenworth, Kansas 66027				8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Command and General Staff College Fort Leavenworth, Kansas 66027				10. SPONSORING / MONITORING AGENCY REPORT NUMBER
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT  APPROVED FOR PUBLIC RELEASE: DISTRIBUTION UNLIMITED.				12b. DISTRIBUTION CODE
13. ABSTRACT (Maximum 200 words) SEE ATTACHED				
14. SUBJECT TERMS Nonlethal Psychological operations Information Operations Targeting				15. NUMBER OF PAGES 62
				16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UNLIMITED	

**THE NONLETHAL INFORMATION  
OPERATIONS TARGETING PROCESS:  
DUTIES, RESPONSIBILITIES AND  
PROCEDURES**

**A MONOGRAPH  
BY  
Major Erin J. Gallogly-Staver  
Military Intelligence**

**School of Advanced Military Studies  
United States Army Command and General Staff  
College  
Fort Leavenworth, Kansas**

**First Term AY 98-99**

Approved for Public Release Distribution is Unlimited

**DTIC QUALITY INSPECTED 2**

19990804 050

SCHOOL SCHOOL OF ADVANCED MILITARY STUDIES

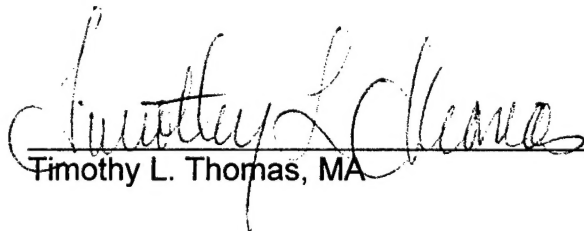
MONOGRAPH APPROVAL

Major Erin J. Gallogly-Staver

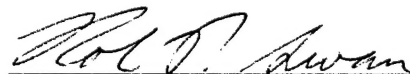
Title of Monograph: *The Nonlethal Information Operations Targeting Process:*

*Duties, Responsibilities and Procedures*


Approved by:

  
Timothy L. Thomas, MA

Monograph Director

  
LTC Robin P. Swan, MMAS

Director, School of Advanced  
Military Studies

  
Philip J. Brookes, Ph.D.

Director, Graduate Degree  
Program

Accepted this 16th Day of December 1998

## ABSTRACT

**THE NONLETHAL INFORMATION OPERATIONS TARGETING PROCESS: DUTIES, RESPONSIBILITIES, AND PROCEDURES** by MAJ Erin J. Gallogly-Staver, USA, 55 pages.

Many articles, journals, and books describe what information operations are and how they are essential to military operations, but there is little written about how to actually do information operations. This monograph's purpose is twofold. First, it provides the Joint Task Force Commander procedures by which to integrate nonlethal information operations into the joint targeting process and recommends duties and responsibilities for staff officers to ensure they integrate information operations into plans and operations. Second, it offers information operations officers a single document from which to develop standing operating procedures and tactics, techniques, and procedures.

Joint Publications 3-0, *Doctrine for Joint Operations*, and 3-09, *Doctrine for Joint Fire Support*, provide the doctrinal underpinnings for joint targeting. Additionally, Joint Publication 3-13, *Joint Doctrine for Information Operations*, provides doctrine and guidance for information operations targeting. Currently there is neither Army doctrine for information operations targeting nor tactics, techniques, and procedures on how to integrate information operations into the targeting process. This monograph attempts to fill this gap.

The capabilities, limitations, and employment considerations are outlined for the nonlethal information operations capabilities and activities (i.e., civil affairs, electronic warfare, military deception, psychological operations, public affairs, and special information operations). Finally, the author makes several recommendations in the areas of personnel and organization, training and education, doctrine, and operations.

## TABLE OF CONTENTS

I.	INTRODUCTION AND BACKGROUND .....	1
II.	NONLETHAL INFORMATION OPERATIONS CAPABILITIES AND EFFECTS .....	9
III.	DUTIES, RESPONSIBILITIES, AND PROCEDURES.....	26
IV.	CONCLUSIONS, RECOMMENDATIONS, AND IMPLICATIONS .....	40
	ENDNOTES .....	47
	BIBLIOGRAPHY .....	52

## I: INTRODUCTION AND BACKGROUND

Our military must be skilled in the use of bytes and bayonets alike.<sup>1</sup>

Joint Publication 1

Many articles, journals, and books describe what information operations are and how they are essential to military operations, but there is little written about how to actually do information operations. This monograph's purpose is twofold. First, it provides the Joint Task Force Commander procedures by which to integrate nonlethal information operations into the joint targeting process and recommends duties and responsibilities for staff officers to ensure they integrate information operations into plans and operations. Second, it offers information operations officers a single document from which to develop standing operating procedures and tactics, techniques, and procedures.

### **Background and Doctrine**

Joint Publications 3-0, *Doctrine for Joint Operations*, and 3-09, *Doctrine for Joint Fire Support*, provide the doctrinal underpinnings for joint targeting. Additionally, Joint Publication 3-13, *Joint Doctrine for Information Operations*, provides doctrine and guidance for information operations targeting. "Targeting occurs at all levels . . . with both lethal and nonlethal disruptive and destructive means," however, experience demonstrates that nonlethal means are rarely incorporated into the targeting process.<sup>2</sup> Currently there is neither Army doctrine for information operations targeting nor tactics, techniques, and procedures on how to integrate information operations into the targeting process. While Joint Pub 3-13 lists Information Operations Officer functions, experience demonstrates that many information operations officers are unfamiliar with how to

perform those functions. For example, when, where, and how does the information operations officer deconflict targets?

### **Definitions**

This monograph uses the following definitions. **Information Operations (IO)** are actions taken to affect adversary information and information systems while defending one's own information and information systems.<sup>3</sup> **Nonlethal** is a term used broadly to describe capabilities which affect targets temporarily or permanently, without intentionally causing death to personnel or without unnecessary destruction or environmental damage.<sup>4</sup> **Nonlethal information operations** are those capabilities and activities, such as psychological operations (PSYOP), civil affairs (CA), public affairs (PA), electronic warfare (EW), and special information operations (SIO), which have an effect other than death or destruction. Affects of nonlethal information operations include deceive, disrupt, delay, deny, degrade, manipulate, influence, or inform. This monograph will not address nonlethal weapons, such as CS gas, rubber bullets, or sticky foams.

A **joint task force (JTF)** is a force composed of assigned or attached elements of the Army, the Navy or the Marine Corps, and the Air Force, or two or more of these Services, which is constituted and so designated by the Secretary of Defense or by the commander of a unified command, a specified command, or an existing joint task force.<sup>5</sup> For the purposes of this monograph, an Army Corps headquarters functions as the nucleus of the Joint Task Force; the Corps Commander is the Commander, Joint Task Force (CJTF) and other services provide forces as required. The Joint Task Force is functionally organized with a Joint Force Air Component. The Commander establishes a

Joint Targeting Coordination Board; the Deputy Commander or Chief of Staff chairs its meetings. Additionally, the Land Information Warfare Activity (LIWA) and the Joint Command and Control Warfare Center (JC2WC) provide personnel to assist the Joint Task Force with information operations planning. The Joint Staff or Intelligence Community provides personnel to conduct Special Information Operations.

### **Targeting Methodology**

The Army and Marine Corps' Decide, Detect, Deliver, and Assess (D3A) targeting methodology is easily translated into the joint targeting process. (See Figure 1.) Given that Service biases do exist, all planners participating in the joint targeting process must become familiar with it to prevent confusion and misunderstanding. The **joint targeting process** comprises six phases: commander's objectives and guidance, target development, weaponeering assessment, force application, execution planning and force execution, and combat assessment. These phases are iterant and occur nearly simultaneously rather than sequentially.

In Phase One, the Commander establishes objectives and guidance. He "sets priorities, provides targeting guidance, and determines the weight of effort to be provided to various operations."<sup>6</sup> It is critical that objectives and guidance are clear, concise, and quantifiable to ensure planners meet the commander's intent. XVIII Airborne Corps uses task, purpose, method, and desired end state to clarify objectives and guidance.<sup>7</sup> The following example illustrates a way to state objectives and guidance.

Task: disrupt the command and control capability of the insurgents.

Purpose: effect their ability to conduct nightly raids on the host nation radio, television, and power stations.



Method: use of nonlethal information operations attack assets.

Desired End State: uninterrupted host nation broadcasts.<sup>8</sup>

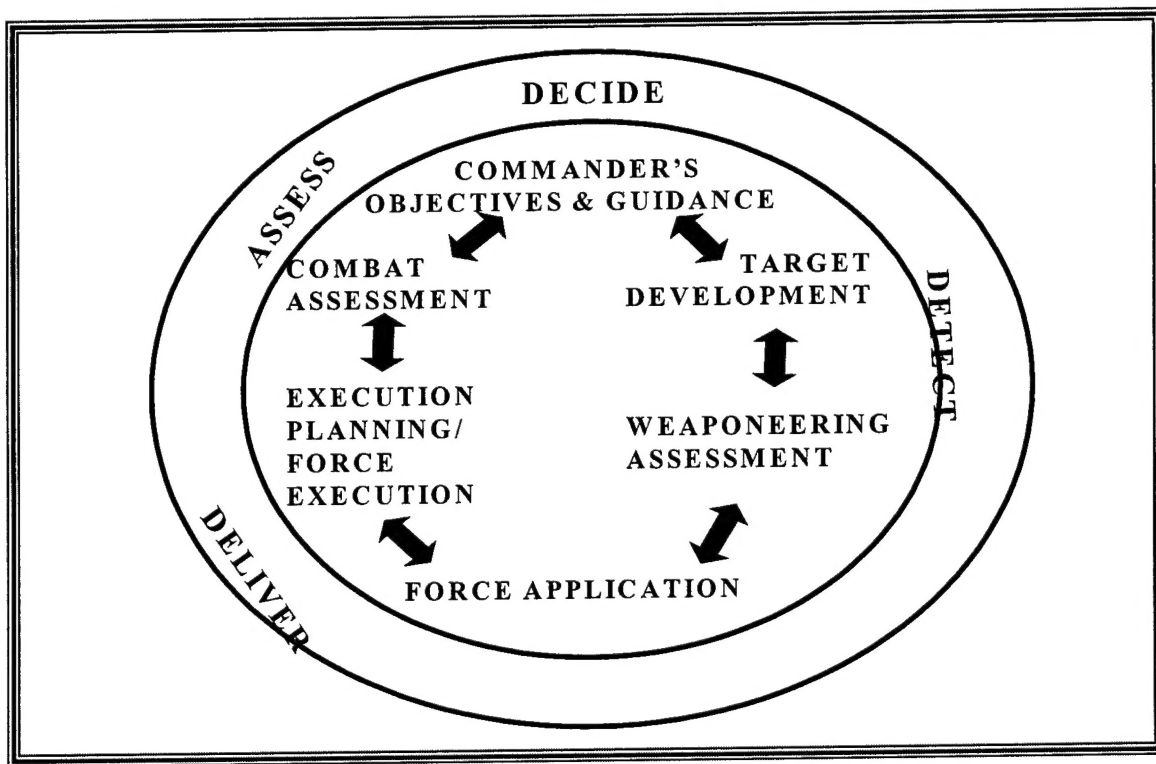


Figure 1. The Army/Marine Corps Targeting Process  
Overlaid onto the Joint Targeting Process<sup>9</sup>

In Phase Two, **target development**, planners and targeteers systematically evaluate potential target systems and their components. Targeteers translate the commander's objectives and guidance into target lists. End products include the Joint Integrated Prioritized Target List (JIPTL), a prioritized list of targets scheduled for attack. It also includes those targets that are not scheduled for attack. Once the joint force commander approves the Joint Integrated Prioritized Target List, the J3 or typically the Joint Force Air Component Commander (JFACC) publishes an Air Tasking Order (ATO).<sup>10</sup>

Targeteers determine the quantity, type, and mix of lethal and nonlethal weapons required to produce a desired effect in Phase Three, **weaponneering assessment**. **Force application**, Phase Four, is the selection of lethal or nonlethal forces for the mission based on the capabilities of the joint force. Phase Four's primary objective is to sequence target attacks and synchronize the application of lethal or nonlethal force. In Phase Five, **Execution planning and force execution**, component commanders and staffs conduct mission planning and forces execute operations. **Combat assessment**, the final phase, determines the overall effectiveness of force execution.<sup>11</sup>

### **Information Operations Overview**

Information operations should be an integral part of all joint military operations.<sup>12</sup> Figure Two depicts a typical joint information operations cell. The cell coordinates information operations capabilities and activities in all joint force planning activities. Experience shows that while a cell may exist, its members often lack expertise. Additionally, there is a lack of tactics, techniques, and procedures (TTP) that outline how to employ information operations as an "integrating strategy."<sup>13</sup>

The Army's doctrinal manual on information operations (Field Manual 100-6, *Information Operations*) does not discuss targeting. A representative from the information operations cell provides input to the joint targeting coordination board (JTCB).<sup>14</sup> Offensive information operations target three areas: human factors (e.g., commanders, troops, population groups), links (e.g., conduits through which information flows, such as telephone lines), and nodes (e.g., processors, physical plants, satellites). These target areas are sometimes referred to as hard (i.e., things) and soft (i.e., people).

Planners require detailed intelligence on both hard and soft targets when integrating and deconflicting information operations with other operations.

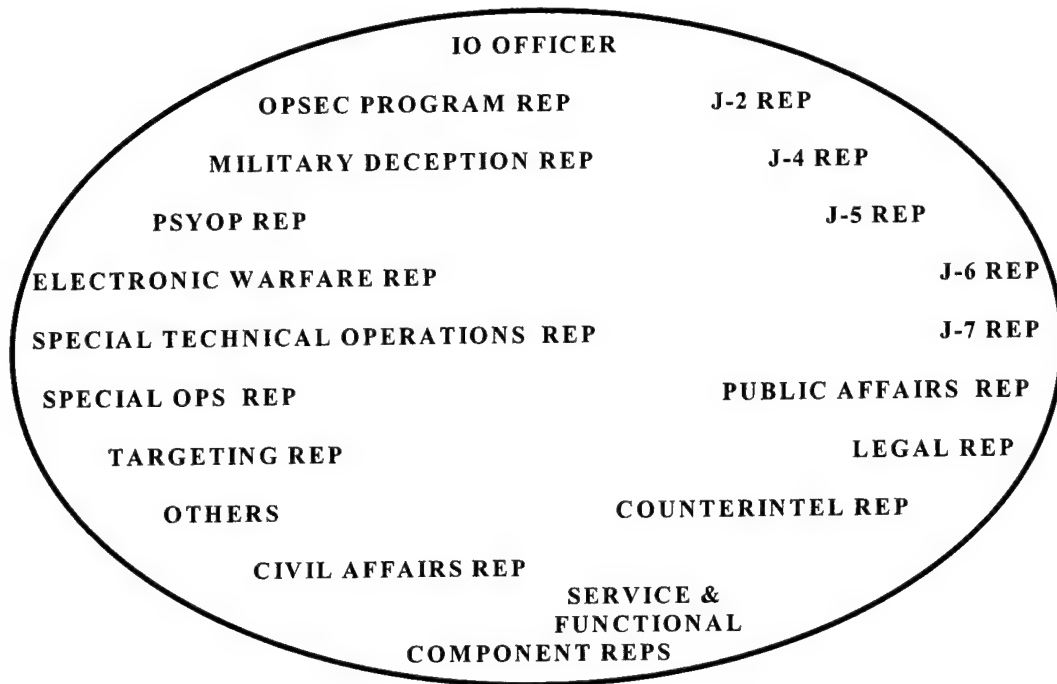


Figure 2. Typical Joint Information Operations Cell.<sup>15</sup>

### Evaluation Criteria<sup>16</sup>

Planners and targeteers use thirteen principles when planning fire support, which provide a way to measure the effective use of available fire support resources. When the information operations officer conducts planning, he should employ these principles as appropriate to nonlethal information operations. This monograph uses seven of the principles to demonstrate how planners can integrate nonlethal information operations into the joint targeting process.

#### Plan Early and Continuously

“To effectively integrate fire support with the scheme of maneuver, planning must begin when the commander states the mission and provides command guidance.” The

first phase in the joint targeting process is to establish objectives and guidance. It is during this phase that the information operations officer should develop information operations-specific objectives and guidance. As the situation changes, he recommends changes to those objectives and guidance.

#### Consider the Use of all Lethal and/or Nonlethal Attack Means

“Fire support planners and/or coordinators consider all attack means available at their level and higher levels.” Experience and history demonstrate that this principle receives cursory attention. The majority of fire support planning involves lethal means. New information-age technologies and classical nonlethal capabilities, such as psychological operations and military deception, should receive equal attention by fire support and other planners. This point is even more relevant during the conduct of military operations other than war (MOOTW).

#### Use the Most Effective Fire Support Means

“The fire support planners and/or coordinators should consider the nature and importance of the target, the engagement time window, the availability of attack assets, and the results desired . . . . it may be necessary to use multiple assets to achieve the desired effects on a target.” Synergy occurs when the whole is greater than the sum of its parts, exactly the case when planners integrate, synchronize, and deconflict lethal and nonlethal fires. The combined effects of B-52 bombs and leaflet drops on the Iraqi front line troops during the Persian Gulf War demonstrate this important principle.

#### Coordinate Airspace and Protect the Force

“Effective airspace management requires a responsive airspace control system, standardization, minimal restrictions, and continuous coordination among all airspace

users . . . . given the complexity inherent in joint fire support, prevention of fratricide must always be a high priority.” As more and more assets from diverse organizations use the airspace, it is imperative that airspace coordination occur to prevent fratricide. Planners should develop procedures to coordinate and deconflict lethal aircraft, such as A-10s and B-52s, nonlethal aircraft, such as the EC-130E Commando Solo, and unmanned aerial vehicles (UAVs), long-range artillery, such as ATACMS, and precision guided missiles, such as sea-launched Tomahawk cruise missiles. Planned and ad hoc missions may have different procedures; however, the goal is to prevent fratricide.

#### Provide Adequate Support

“Fire support planners and/or coordinators must conserve capabilities by ensuring that only the minimum force needed to achieve the desired effects is used.” This principle complements the principle of considering all means available. Perhaps nonlethal information operations capabilities and activities would achieve the desired effects in a less-costly manner than lethal force. Planners must judiciously employ capabilities in a resource-constrained environment.

#### Provide for Flexibility

“Fire support planners and/or coordinators must anticipate and provide for future contingencies. On-order missions and the careful positioning of assets give the commander the flexibility to respond to changing battlefield conditions.” This principle coupled with the previous principle reiterates the need to consider all means available. If one type of operation does not result in success then perhaps another type would be more effective. Considering and planning for all available means allows the commander to employ a variety of options.

## **II: NONLETHAL INFORMATION OPERATIONS CAPABILITIES AND EFFECTS**

Wisdom is better than force.  
Ecclesiastes 9:13

There are many nonlethal information operations attack assets available to the Joint Task Force. The information operations officer must understand the capabilities, limitations, and employment characteristics of these assets in order to fully synchronize and leverage their potential. Figures 3 through 6 depict nonlethal attack assets available at Corps with its subordinate units and components, and higher. Figure 7 describes nonlethal capabilities that may be available to a Joint Task Force in the future. Figure 8 also offers descriptions of nonlethal information operations effects. Those descriptions should be included in future doctrinal information operations and targeting publications. These definitions provide a common framework from which to plan, execute, and evaluate the use of nonlethal information operations.

### **Information Operations Officer and Information Operations Cell**

The J-3 will normally designate an information operations officer to coordinate information operations for the joint force commander.<sup>17</sup> He supervises the information operations cell discussed in Chapter I (see Figure 2). Currently, the information operations officer is not a modified table of organization and equipment (MTOE) position. Therefore, incumbents are typically the psychological operations officer, command and control warfare officer, or a J3 staff officer with information operations-type experience. Under the U.S. Army's Officer Personnel Management System XXI (OPMS XXI), officers can designate their career field as functional area 30, Information Operations. To date a board has not selected officers to serve as information operations

officers. Therefore, any branch or functional area officer may serve as an information operations officer in the interim. For example, a field artillery (Branch 13) or a psychological operations (Functional Area 39B) officer may serve as the information operations officer. As previously stated this officer should receive training and education germane to information operations. Often, however, he has no experience when appointed.

The information operations cell consists of representatives from the following staffs and organizations.

- \* Joint force's staff.
- \* Higher level staffs (e.g., the Joint Staff).
- \* Service and functional component commands [e.g., the Joint Psychological Operations Task Force (JPOTF) or Joint Forces Psychological Operations Component Command (JFPOCC)].
- \* Subordinate information operations cells.
- \* Department of Defense agencies (e.g., Defense Intelligence Agency).
- \* Joint centers (e.g., Joint Command and Control Warfare Center).

Some representatives are permanent or resident members of the cell while others are nonresident members and participate as required. For example, the psychological operations representative would be a resident member, whereas the legal representative would be a nonresident member. The composition and disposition of the cell are mission-dependent, but the information operations officer should seek to maximize participation by all members to ensure synchronized and deconflicted operations. The cell is a staff organization, not an operational element. Hence, the cell does not conduct information operations; rather it maximizes capabilities and activities by coordinating and deconflicting information operations.<sup>18</sup>

## **Nonlethal Information Operations Attack Assets**

Nonlethal information operations capabilities and activities used in offensive information operations include civil affairs, military deception, electronic attack, psychological operations, public affairs, and special information operations. Those information operations that contribute to offensive information operations, such as operations security, or are lethal, such as physical destruction, are not discussed here.

### **Civil Affairs**

Civil Affairs activities support the commander's relationship with civil authorities and the civilian populace in the area of operation. Civil-military operations and support to civil administration are the two missions of civil affairs units. Civil-military operations include populace and resource control, foreign nation support, humanitarian assistance, military civic action, and civil defense. Civil assistance, to include technical expertise in twenty functional area specialties, and civil administration in friendly or occupied territories comprise support to civil administration operations.<sup>19</sup> Typically, civil affairs units establish a Civil-Military Operations Center (CMOC) to synchronize and deconflict their operations. A civil-military operations center normally has four sections: headquarters, operations, administrative and logistics, and other representatives, such as psychological operations specialists, nongovernmental organizations, and host nation officials.

The majority of civil affairs units are in the U.S. Army. Over ninety-six percent of Army civil affairs units are in the Reserve Component. The U.S. Marine Corps recently activated two Reserve Component civil affairs units: the 3<sup>d</sup> and 4<sup>th</sup> Civil Affairs Groups. In a Major Theater War, a Marine Reserve Group would mobilize and deploy



with a Marine Air Ground Task Force (MAGTF) command element to assist with dislocated civilians, conduct public health and welfare functions, and conduct liaison with non-military organizations.<sup>20</sup> An Army Reserve Component civil affairs brigade will normally support a Corps-sized Joint Task Force. Subordinate to the brigade are general-purpose civil affairs battalions composed of a variety of civil affairs teams.

Figure 3 describes various civil affairs elements.

TYPE TEAM	TYPE SUPPORT	TEAM SIZE
Civil Affairs Tactical Headquarters Support Team (CATHST)	Provides support to maneuver battalion, brigade, and division staff; can augment a JTF or JSOTF staff.	6
Civil Affairs Tactical Support Team (CATST)	Provides support to maneuver battalions, brigades, and divisions; can augment a JTF or JSOTF staff.	AC: 4 RC: up to 6
Civil Affairs Plans, Programs, and Policy Team (CAP3)	Provides support to Unified Commands.	RC: 10
Civil Affairs Operational Planning Team (CAOPT)	Provides support to theater service and/or functional components.	5
Civil Affairs Tactical Planning Team (CATPT)	Provides planning support to maneuver units up to Corps and JTF level.	5
Civil Affairs Language Team (CALT)	Provides language support to all levels.	RC: 5
Civil Affairs General Support Detachment (CAGSD)	Provides support to maneuver, CS, and CSS units.	RC: up to 15
AC: Active Component      CS: Combat Service      CSS: Combat Service Support JTF: Joint Task Force      JSOTF: Joint Special Operations Task Force RC: Reserve Component		

Figure 3. Civil Affairs Elements<sup>21</sup>

Civil affairs units have the following capabilities:<sup>22</sup>

- \* Provide staff augmentation and civil affairs planning and assessment support.
- \* Plan and support civil-military operations conducted by military forces.
- \* Minimize civilian interference.
- \* Promote legitimacy.
- \* Conduct liaison with host nation organizations, nongovernmental organizations, and U.S. government agencies.

- \* Identify civilian resources to support the mission.
- \* Support civil administration with technical expertise and advice.
- \* Provide linguistic, regional, and cultural expertise.

Limitations of civil affairs units include their requirement for external support, such as logistics, lodging, fueling, and the time required to deploy Reserve Component forces. Employment considerations are minimal. The Civil-Military Operations Center should be co-located with the Joint Task Force headquarters outside of any secured classified area. For a Civil Military Operations Center supporting a Joint Task Force a building with electrical power is preferable; however, two Standard Integrated Command Post tents and a 3.2-kilowatt generator will suffice.

### Military Deception

Military deception are actions executed to mislead opposing decisionmakers, causing them to derive and accept desired appreciations of military capabilities, intentions, operations, or other activities that evoke actions contributing to the originator's objectives.<sup>23</sup> The Land Information Warfare Activity (LIWA) provides deception planning support to Land Component and separate Army commands, whereas the Joint Command and Control Warfare Center (JC2WC) provides deception planning support to joint forces. Only time, physical space, and the competence and imagination of the deception planner constrain a force's ability to conduct military deception. The deception staff officer (DSO) at Corps is the primary deception planner for the joint task force. While there is formal training available for deception planners, most deception staff officers have not received it. The majority of training occurs on-the-job during field exercises and command post exercises. The U.S. Army no longer has soldiers trained to conduct deception operations. In October 1998, the Military Intelligence community

eliminated Military Occupational Specialty 97G, Deception Specialist, and the associated units trained and equipped to plan for and execute deception operations.

The doctrinal manual for military deception (Field Manual 90-2, *Military Deception in Army Operations* (Draft)) has been in revision for nearly a decade. The current draft states it “focuses on the tactical level of military operations, specifically military deception in support of Echelons Corps and Below (ECB), as well as joint task force Army Force (ARFOR) operations.”<sup>24</sup> However, it lacks guidance on how to execute deception operations in a resource-constrained environment. The manual does offer a methodology for planning deception operations and historical examples to demonstrate the potential gains of a coordinated, resourced, and synchronized deception plan.

The Joint Task Force will likely receive augmentation from the Joint Command and Control Warfare Center or the Land Information Warfare Activity. Additionally, personnel from the Joint Staff, combatant command, or from the intelligence community’s special information operations elements will provide available resources to assist the deception planner. Employment considerations include balancing the need to coordinate and synchronize operations with the need to maintain security of the deception plan.

### Electronic Attack

Electronic attack is that division of electronic warfare involving the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Electronic attack includes nondestructive actions, such as jamming and

electromagnetic deception, and employs weapons, such as lasers, radio frequency weapons, and particle beams, to prevent or reduce an enemy's effective use of the electromagnetic spectrum.<sup>25</sup> This monograph considers only nonlethal electronic attack operations, such as jamming and deception.

The joint force commander has several nonlethal electronic attack assets available. Figure 4 describes the capabilities of those systems. In addition to range limitations, planners must consider frequencies used by military forces to operate and also consider frequencies exploited for intelligence or other operations, such as psychological operations or deception. Electronic warfare units receive the Joint Restricted Frequency List (JRFL), which are those frequencies that friendly forces do not want to jam.

ELECTRONIC ATTACK ASSET	CAPABILITY
AN/ALQ-151 QUICKFIX (EH-60A Blackhawk helicopter)	Airborne jammer targeted against tactical single channel communications at battalion and regimental level. VHF bandwidth (1.5MHz-150MHz)
AN/TLQ-17 TRAFFICJAM	Ground-based jammer targeted against communications at battalion and regimental level. HF/VHF bandwidth (20-80 MHz). (To be replaced by Ground Based Common Sensor functions.)
EA-6B PROWLER	Carrier-based airborne communications jammer. VHF/SHF bandwidth (64MHz-18GHz). (AN/ALQ-149 & AN/ALQ-99)
EC-130H COMPASS CALL	Airborne noise jammer. HF-UHF (20MHz-1640MHz)
EF-111 RAVEN	Airborne non-communications (radar) jammer. (AN/ALQ-99)

Figure 4. Electronic Attack Assets.<sup>26</sup>

Employment considerations are minimal, but essential. All airborne electronic attack assets that operate in the Joint Operations Area should appear on the Air Tasking Order. It provides useful information required to deconflict and synchronize operations and is not simply a "tasking order". Planners must also consider logistics issues such as airstrip landing capacity, on-station time limits, and refueling requirements.

### Psychological Operations

Psychological operations (PSYOP) are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. Doctrinally, psychological operations induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.<sup>27</sup>

While all military actions have a psychological affect, not all military operations are psychological operations. This concept is not always obvious. For example, with the advances in information technology, such as desktop publishing computers and color printers, military units other than psychological operations units may attempt to conduct psychological operations. Well-meaning commanders may unintentionally commit a faux pas as a result when disseminating products. Psychological operations personnel receive specialized training in target audience analysis and are well-versed in the cultural mores and norms of foreign audiences. Any attempt by personnel other than psychological operations personnel to conduct psychological operations should be avoided, especially since uncoordinated products could negatively affect the theater psychological operations campaign.

All military psychological operations capabilities are in the U.S. Army save the EC-130E Commando Solo, an airborne dissemination platform, located in the Air National Guard. Psychological operations units develop, produce, and disseminate audio, visual, audio-visual, and printed products. Military and civilian psychological operations and intelligence specialists develop products based on target audience analysis. Figure 5 describes psychological operations production and dissemination assets.

PSYOP ASSET	CAPABILITY
Modular Print System (MPS)	Capable of producing black & white or color print products.
Heavy Print Plant	Fixed facility to produce large quantities of multi-color or photographic products.
Deployable Product Production Center (DPPC)	Graphics computer with limited color digital printing capable of reproducing pre-approved products in limited quantities. Limited audio production.
Deployable Audio Production System (DAPS)	Audio production on cassette, compact disk, or mini-disk.
Deployable Digital Video Edit System (Fly-Away AVID)	TV production capability using BETA PAL/NTSC, multistandard VHS, and HI-8.
MSQ-85B Audio-visual unit	Audio, visual, and audio-visual production and dissemination. Can produce audio-visual presentations, photographic slides, loudspeaker broadcasts, and limited leaflet production.
PSYOP Airmobile Dissemination System (PAMDIS)	Capable of broadcasting AM, FM, and/or television (530-1605KHz; 97.5MHz, Channel 5 or 7); range is 50km for AM and 15-20km for FM and TV. Mobile configuration: AM, FM, & TV. Modular configuration: FM & TV
Portable AM Transmitter-400 watt (PAMT-400)	Capable of live or pre-recorded broadcasts in 1000-1650KHz bandwidth or retransmission; range is 35km.
Special Operations Media System B (SOMS-B)	Mobile medium range AM/FM/TV broadcast capability. Digital video and audio editing and tape duplication. Ranges: AM (80km), FM (25km), SW (480km), VHF (TV) (6km). Mounted on two HMMWVs with attached tents and two support HMMWVs.

Transportable AM Transmitter-10kw (TAMT-10)	Capable of radio transmission, reception, and production. Broadcast from 535-1705KHz; range is 80km.
Transportable AM Transmitter-50kw (TAMT-50)	Capable of broadcasts in 535-1620 KHz; range is 160km.
Portable FM Transmitter-1000 watt (PFMT-1000)	Capable of broadcasts in 87.5-108KHz; range is 33-46km.
Portable FM Transmitter-2000 watt (PFMT-2000)	Capable of broadcasts in 87.5-108KHz; range is 43km.
TSQ-171 (TV-T5) Television Transmitter-5KW	Capable of TV broadcasts (174-216MHz; channels 7-13 for NTSC & 5-10 for PAL/SECAM); range is 70-120km.
Loudspeakers	Man-packed, vehicle- or helicopter-mounted broadcast platforms with range from 700-1800 meters.
M129E1/E2 Leaflet bomb	Holds approximately 60-80,000 leaflets; dropped from A-6, A-10A, B-52H, F-15E, F-16A-D, F/A-18, F-111D-F aircraft.
Leaflet boxes	Standard copier paper box holds approximately 20,000 leaflets; dropped from any fixed or rotary wing aircraft that can be rigged to accommodate a static line.
EC-130E Commando Solo	An airborne electronic broadcasting platform capable of broadcasting AM/FM radio, television, short-wave and military communication bands.

Figure 5. Psychological Operations Production and Dissemination Assets<sup>28</sup>

The major limitations of psychological operations units are:

- \* The lengthy approval process.
- \* The challenges associated with the inability to effect early coordination.
- \* The challenges associated with Reserve Component mobilization.
- \* The requirement for combat support and combat service support from

the Army Service Component Command (ASCC) or Theater Army Special Operations Support Command (TASOSC).

\* The requirements for transportation and dissemination support from U.S. Army aviation units and the U.S. Air Force.

There are many employment configurations for psychological operations forces. Elements range from a three-person tactical psychological operations team (TPT) (i.e., loudspeaker team) to a Group-sized Psychological Operations Task Force (POTF). A multi-battalion-sized Joint Psychological Operations Task Force (JPOTF) normally deploys in support of a Joint Task Force. Elements from the tactical, regional, and dissemination psychological operations battalions will task organize to form a JPOTF under the command and control of either a battalion or group commander. Psychological operations elements are attached to the Joint Task Force and subordinate units down to brigade level to provide staff planning and supervision of subordinate tactical elements. Approximately thirteen to sixteen personnel comprise these elements called Tactical PSYOP Detachment, Tactical PSYOP Development Detachment, Tactical PSYOP Company, and Tactical PSYOP Battalion [formerly called Brigade, Division, and Corps Psychological Operations Support Elements (BPSE, DPSE, and CPSE)]. Each element has limited audio and print development and production capability; additionally, each Tactical PSYOP Company and Battalion has one aerial loudspeaker system. Typically, the Detachments and Company tailor and reproduce pre-approved products in support of their maneuver unit.

#### Public Affairs

Public affairs are those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense.<sup>29</sup> Figure 6 depicts a typical joint task force public



affairs organization capable of performing core public affairs functions: media relations, command information, community relations, and planning. “An information bureau is a single point of interface between the military and news media representatives covering military operations. Command information involves informing the various internal audiences about the participation of military forces in joint operations.”<sup>30</sup> Community relations include relations with both home station and deployed communities.

When deployed, civil affairs personnel are responsible for relations with local populations; however, public affairs personnel may support civil affairs operations. The Public Affairs Officer develops public affairs guidance (PAG) for the joint task force commander; the Assistant Secretary of Defense for Public Affairs [ASD(PA)] approves it. The guidance establishes a clear set of facts and tenets, serves as a source document in responding to news media, and provides a mechanism to coordinate public affairs, civil affairs, and psychological operations messages.

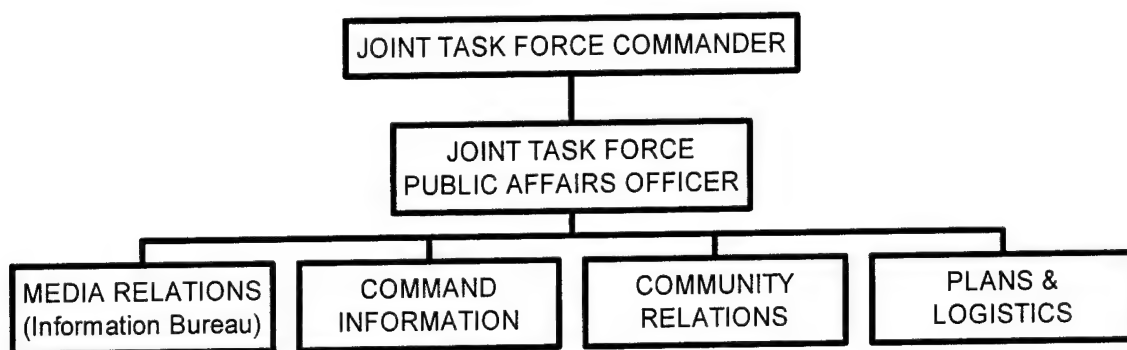


Figure 6. Joint Task Force Public Affairs Organization<sup>31</sup>

Limitations of public affairs units are major and include the need for combat service and combat service support, such as personnel, transportation, and communications and technical resources. The supported commander and/or the Service

components provide these resources for both the public affairs units and the accompanying media personnel. These requirements are often extensive and should be identified as early in the planning process as possible.

Public affairs assets include a wide-range of capabilities from a sole Public Affairs Officer to a Public Affairs Operations Center (POAC). Like civil affairs units, the majority of public affairs units are in the Reserve Component of the U.S. Army. In the Army, every echelon brigade and above has an organic public affairs section to provide public affairs support and to conduct public affairs planning and operations. A Public Affairs Detachment (PAD) is the smallest table of organization and equipment (TOE) unit that provides direct public affairs support; the Corps assigns PADs to support divisions, brigades, regiments, and special operations forces. A Broadcast Operations Detachment (BOD) conducts internal information broadcast services; there is one BOD per Public Affairs Operation Center (POAC). Mobile Public Affairs Detachments (MPAD) are found at joint task force, corps, and division levels. The Public Affairs Operation Center, found at corps and above, commands and controls all attached MPADs, BODs, and PADs.

#### Special Information Operations

Special information operations (SIO) “are operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to U.S. national security, requires a special review and approval process.”<sup>32</sup> The Corps should also have its own separate Special Technical Operations officer to facilitate coordination with other Components and Department of Defense agencies through the Planning and Decision Aid System (PDAS). The level of responsibility and access required by the

special technical operations officer may preclude the information operations officer from devoting his full attention to information operations planning with special technical operations as an additional duty. However, the Joint Staff, Joint Command and Control Warfare Center (JC2WC), the Joint Warfare Analysis Center (JWAC), or the Land Information Warfare Activity (LIWA) can provide assistance if necessary. Regardless, the information operations officer must be familiar with the capabilities, limitations, and approved operations of any element that provides information operations support to the joint force commander. These elements can provide him limited access so that he can properly advise the joint force commander and ensure these special information operations are deconflicted with other operations. Employment considerations include balancing the need to coordinate and synchronize operations with the need to maintain security.

The joint task force information operations officer may also request and receive support from the following joint activities and Department of Defense agencies:

- \* Joint Command and Control Warfare Center (JC2WC)
- \* Joint Warfare Analysis Center (JWAC)
- \* Joint Program Office for Special Technology Countermeasures (JPO-STC)
- \* Joint Staff, Special Technical Operations Division (STOD)
- \* Joint Spectrum Center (JSC)
- \* National Security Agency (NSA)
- \* Defense Intelligence Agency (DIA)
- \* Defense Information Security Agency (DISA)

### **Future Nonlethal Technologies**

There are many nonlethal technologies under development or research by commercial businesses, foreign governments, and non-state actors. Appearance on this list does not necessarily indicate that the Department of Defense is developing these

capabilities. Some nonlethal technologies that the information operations officer should consider for futuristic information operations include those found in Figure 7.

<b>PERSONNEL &amp; MATERIEL EFFECTORS</b>	<b>DESCRIPTION</b>	<b>POSSIBLE NONLETHAL IO EFFECTS</b> (see Figure 8)
Infra/Ultra Sound	Sonic generator that projects an acoustic pressure wave to cause discomfort to personnel.	Confuse, degrade, disable
Noise	Acoustic generator that produces sufficient sound to disorient or incapacitate personnel.	Disable, influence.
Incapacitating Substances	Family of inorganic and organic substances that cause temporary disability.	Disable, physical effects.
Holograms	Generator that produces holograms as decoys or deceptions.	Manipulate, threaten.
Voice Synthesis or Morphing	Device to synthesize the voice or images of a known figure to deceive, produce false orders, or gain access.	Deter, manipulate.
Special Electromagnetic Interference	Family of devices that provide electronic interference effects.	Degrade, deny.
High-Voltage Shock	High-voltage generator that disrupts electronic systems.	Degrade, delay, deny.
Nonnuclear EMP	Device that duplicates the effects of nuclear weapons electromagnetic pulse, disrupting electronics.	Degrade, delay, deny.
Conductive Particles & Ribbons	Family of particles and ribbons that short-circuit electronics when inserted or deployed over wires.	Degrade, deny, disorganize.
Radio Frequency	System that radiates a microwave burst, disabling electronics.	Degrade, deny.
Optical Munitions	Explosive or electric flash device to stun, dazzle, or temporarily blind optical sensors.	Confuse, disorganize, physical effects.
Computer Moles, Worms, & Viruses	Family of programs that will burrow into enemy automation and report back various datum or cause malfunction.	Influence, manipulate, mislead.
Environmental	Family of technologies that cause changes in the physical environment, such as changes in weather patterns.	Delay.

Figure 7. Personnel and Materiel Effectors.<sup>33</sup>

### Nonlethal Information Operations Effects

Lethal fires express effects both subjectively and quantifiably. The traditional effects of fires—harass, suppress, neutralize, and destroy—are subjective; however, commanders typically issue guidance to quantify them. For example, destroy thirty percent of artillery and seventy percent of maneuver forces or conduct suppression fires for thirty minutes at H+1.

Currently, there are no nonlethal information operations effects in doctrine. While practitioners of information operations use terms in an attempt to articulate effects, the terms are often subject to individual interpretation. This lack of a common understanding leads to misuse of assets or unrealistic expectations. Figure 8 offers possible definitions for nonlethal information operations effects. Although most of the definitions are not quantified, the information operations officer could establish desired effects for a given time, event, and/or location to meet an information operations objective. The desired effects should flow from the commander's goals and objectives. For example, if the commander joint task force has an objective to *deter country X's aggression*, an information operations objective may be to *reduce country X's leadership's confidence in its armed forces*. Some effects of information operations in support of this objective may include *degrade enemy's early warning capability* or *influence military leaders to cease resistance*. Given certain desired effects the information operations planner can determine how to best achieve them. For example, conduct electronic attacks and psychological operations to degrade the enemy's early warning capability.

<b>NONLETHAL IO EFFECTS</b>	<b>DEFINITION</b>
COMPEL	To force, drive, or constrain; to obtain or bring about by force (or threat of force).
CONFUSE	To perplex; to mistake one thing for another.
DECEIVE	To mislead.
DEGRADE	To reduce in grade; to reduce or divert.
DELAY	To cause to be late or detained.
DENY	To prohibit the use of something.
DETER	To prevent or discourage someone from acting by means of fear or doubt.
DISABLE	To weaken or destroy the normal physical or mental abilities; incapacitate.
DISORGANIZE	To destroy the organization, systematic arrangement, or unity of; throw into confusion.
EXPLOIT	To employ to the greatest possible advantage.
INFLUENCE	Power to sway or affect based; to have power over.
INFORM	To impart information.
MANIPULATE	To influence or manage shrewdly or deviously.
MISLEAD	To lead or guide in wrong direction; to lead into error or wrongdoing in action or thought.
SHAPE	To cause to conform to a particular form or pattern.
THREATEN	To express a threat against.
PHYSICAL EFFECTS	To cause a target to react physically, such as becoming nauseous, paralyzed, or blind.

Figure 8. Nonlethal Information Operations Effects.<sup>34</sup>

### **Timing**

Understanding current and possible future nonlethal information operations capabilities and technologies is just the beginning. The information operations officer must synchronize those capabilities to achieve a desired effect at the appropriate time and location against the right target. This chapter provides the information operations officer a point of reference from which to begin staff planning, coordinating, synchronizing, and deconflicting. The next chapter proposes duties, responsibilities, and procedures by which the information operations officer can effectively and efficiently accomplish his tasks.

### III: DUTIES, RESPONSIBILITIES, AND PROCEDURES

The primary goal of planning is not the development of elaborate plans that inevitably must be changed; but instead is the development of planners who can cope with the inevitable change.<sup>35</sup>

Slide from Joint Planning and Execution Class

Many people from a variety of organizations plan for and conduct the individual capabilities and activities comprising information operations. The Commander, Joint Task Force needs at least one person on his staff—his information operations officer—to advise him on the capabilities, limitations, and employment considerations of information operations. This chapter recommends procedures by which the information operations officer can integrate nonlethal information operations into the targeting process. It also recommends duties and responsibilities for the information operations officer. The evaluation criteria assess whether the recommended procedures, duties, and responsibilities are doctrinally sound.

Figure 9 depicts the critical organizations and products involved in the joint targeting process. The information operations (IO) cell (in this example the IO cell is subordinate to the J3-IO Directorate) recommends information operations-specific goals and objectives to the Battlefield Management Cell (BMC)/Joint Planning Group (JPG). The information operations representative on the Joint Targeting Coordination Board (JTCB) is a voting member and performs advisory and coordination functions. The Component Commands and some Joint Task Force staff sections send representatives to the information operations cell. Some nonresident members, such as from the Staff Judge Advocate, perform advisory functions, while other resident members, such as the J2 representative provide information used in the targeting process.

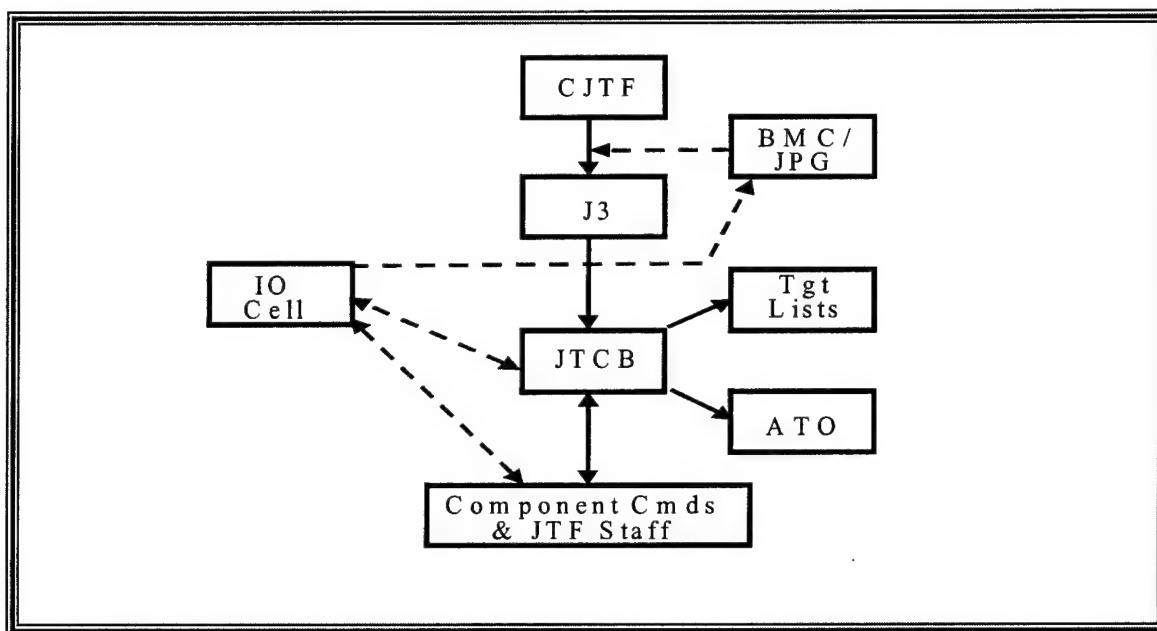


Figure 9. Critical Organizations and Products.

### **Joint Targeting Methodology and Nonlethal Information Operations**

When a Corps forms the nucleus of a Joint Task Force, it uses the six-phased Joint Targeting Methodology discussed in Chapter One. The information operations officer must be familiar with the process, its products, and the organizations and personnel involved. Prior to Phase One the information operations officer must determine the receptivity of the target.

#### **Phase Zero: Receptivity Determination**

Receptivity is a measurement of the target's willingness and ability to receive information operations. If the target, such as a clan leader or its members, is minimally receptive to information operations then the information operations officer should advise the commander of that fact.

In a time-constrained planning environment the information operations officer may use social order as a partial measurement of the group's receptivity. There are three



types of social order: rule of the clan (e.g., Sudan, Somalia, Chechnya), rule of law (e.g., the U.S., Great Britain), or rule of man (e.g., Russia, Iraq). The dedication of an individual group member is closely related to the group's social order. Members of a group with a clan social order are typically more dedicated to their group than members of a rule of law group. Similarly, members of a group with a rule of law social order are typically more dedicated to their group than members of a rule of man group.

The second part of receptivity is to determine if the target can receive nonlethal information operations. If the target does not have radios then they will not be able to receive radio broadcasts; if civil affairs do not occur in the region where the target is located, the operations will be ineffective. After conducting this assessment of a target's receptivity, the information operations officer can advise the commander whether the group will be highly, moderately, or minimally receptive to information operations. With additional time, the information operations officer can conduct a more detailed analysis of a target's receptivity.

#### Phase One: Objectives and Guidance

In phase one the information operations officer should recommend information operations-specific objectives derived from the joint task force objectives. He also should recommend that the commander issue guidance pertinent to the use of information operations. The commander's guidance may indicate that nonlethal capabilities and activities should be used prior to initiation of combat operations and integrated with all operations thereafter. The information operations officer should be familiar with the informational Flexible Deterrent Options (FDOs) developed by his theater Commander-

in-Chief (CINC). Political, informational, economic, and military flexible deterrent options attempt to deter, delay, and prevent escalation.

*Procedures for Phase One: Objectives and Guidance*

To influence the objectives and guidance recommended to the commander, the information operations officer should be a consulting member to the Joint Planning Group (JPG) established at the Joint Task Force. Typically, the Joint Planning Group comprises planners from a variety of specialties who receive their education from the Advanced Military Studies Program. Some members are permanent, such as those planners from the G3 Plans or J5 sections. Other members, such as planners from the Joint Fires Element, provide expertise within their specialty area. This group develops objectives and guidance and helps the Commander visualize a plan.

XVIII Airborne Corps established a standing Battlefield Management Cell (BMC) that meets twice weekly. The G3 Plans section runs the Cell and it forms the nucleus of the J5 Plans section when the Corps forms a Joint Task Force. All Cell members, to include the Corps information operations officer, are also members of the Joint Planning Group. The Joint Planning Group and the Joint Targeting Coordination Board are the two most critical organizations within the Joint Task Force with regard to information operations.<sup>36</sup> These two sections have high visibility with the Commander and their outputs literally affect all plans and operations of the joint force.<sup>37</sup>

*Duties and Responsibilities for Phase One: Objectives and Guidance*

The main duty during this phase is to develop information operations objectives and guidance. When developing objectives to present to the Joint Planning Group, the information operations officer should consider the questions in Figure 10.<sup>38</sup>

1. What does the Joint Task Force want to make the enemy do?
2. Who or what is the target?
3. How does the Joint Task Force want to reach its objectives?
4. Why does the Joint Task Force want to reach its objectives?
5. How much does the Joint Task Force want to affect enemy activity?
6. When and for how long does the Joint Task Force want to reach the objective?
7. Where does the Joint Task Force want to affect enemy activity?
8. How much will it cost to achieve the objective and is it worth the cost?
9. What are the constraints that restrict or indicate the use of certain operations?

Figure 10. Defining Objectives.

1. What does the Joint Task Force want to make the enemy do? Lose its ability to command and control.
2. Who or what is the target? Target: Commander, XXX Corps (soft) and information systems from Corps to Division (hard).
3. How does the Joint Task Force want to reach its objectives? Nonlethal information operations capabilities and activities, specifically psychological operations, military deception, and electronic attack.
4. Why does the Joint Task Force want to reach its objectives? To degrade the enemy's ability to counter friendly operations.
5. How much does the Joint Task Force want to affect enemy activity? (Try to quantify). Military leaders are unable to reposition units to respond to friendly ground attack.
6. When and for how long does the Joint Task Force want to reach the objective? From 150001LDEC98 to 150700LDEC98.
7. Where does the Joint Task Force want to affect enemy activity? Along Routes Apple and Kiwi.
8. How much will it cost to achieve the objective and is it worth the cost? Conduct a comparative analysis among lethal means only, nonlethal means only, and a combination of lethal and nonlethal means.
9. What are the constraints that restrict or indicate the use of certain operations? Rules of Engagement or other restrictions directed by the Commander; minimize damage to the civilian infrastructure.

Figure 11. Defining Information Operations Objectives.

Figure 11 provides an example of how an information operations officer may develop information operations objectives. The information operations officer must

thoroughly understand the concept of operations, the intelligence picture, and the lethal and nonlethal means capable and available to meet the proposed objective. Additionally, he must nest the objectives he presents with objectives from higher levels of command. With answers to these questions the information operations officer can articulate how nonlethal information operations objectives can help achieve the desired end state.

#### *Evaluation Criteria for Phase One: Objectives and Guidance*

If the information operations officer can influence the commander's objectives and guidance, he will be able to influence the targeting process. The information operations officer's **early and continuous** involvement in the planning process can ensure that targeteers and other planners consider nonlethal information operations. His participation will also help targeteers to **use the most effective fire support measures** and to **provide adequate support**.

#### Phase Two: Target Development

Phase two is very labor-intensive for the information operations officer and cell. The cell conducts target analysis to recommend targets that meet the commander's objectives and guidance. It assists the targeteers when they develop target priorities to meet the commander's objectives and guidance.<sup>39</sup> The information operations officer nominates and deconflicts targets prior to and during the Joint Targeting Coordination Board (JTCB) meetings. The products of this phase include target nomination lists and strike weapon and asset recommendations.

#### *Procedures for Phase Two: Target Development*

The information operations cell develops targets that meet the Commander's objectives and guidance by refining targets from a variety of prepared generic target lists.

The cell also develops targets not found on prepared target lists. It analyzes these target systems to determine which part of the sub-systems, such as a component or element, to attack. This systems analysis allows the information operations officer to specifically articulate what nonlethal information operations will target, the reason why, what assets are capable and available, and the effects desired. He can also question nominations that may conflict with current or future information operations. During Fuertes Defenses 99, a recent XVIII Airborne Corps joint exercise, a Component Command effectively nominated every integrated air defense system node rather than just those nodes deemed critical. The information operations officer together with supporting Joint Command and Control Warfare Center targeteers helped to identify critical nodes and deconflict targets.<sup>40</sup> Figure 12 depicts examples of how the cell would analyze a target system. Nonlethal information operations may target only one of the elements if analysis reveals that that element, if attacked, would disable the entire system.

SYSTEM	COMPONENTS	ELEMENTS
Air defense system	Command & control; early warning; intercept	Operator; power generator; radar; air defense weapon
Headquarters	Command & control; intelligence; operations; logistics	Operator; computer; communications retransmission; maintenance facility

Figure 12. Example Target System Analysis

Information operations intelligence requirements are often time-intensive or require special intelligence collection assets, such as human intelligence (HUMINT) or measurement and signals intelligence (MASINT). The intelligence representatives must ensure early inclusion in the Joint Task Force's intelligence collection plan. To facilitate intelligence coordination, an intelligence member from the information operations cell

should co-locate with the Joint Task Force intelligence section, specifically at the Joint Intelligence Support Element (JISE) in the Analysis and Control Element (ACE).

After conducting target analysis, the information operations officer validates the targets to ensure they meet the Commander's objectives and guidance. He also coordinates with the component commands to deconflict targets that may inhibit current or future information operations campaigns. He coordinates with the J6 and provides input into the Joint Restricted Frequency List to prevent electronic warfare fratricides. The information officer also advises the Commander of operations that may provide propaganda value to the enemy.

Next, the information operations officer submits prioritized information operations target nominations through the J3 Fires (or equivalent section within the JTF J3) to the Joint Force Air Component. He also forwards a copy to the information operations officer representative in the Joint Air Operations Center.<sup>41</sup> Additionally, the information operations officer at the Joint Task Force would coordinate target nominations with the Component Command information operations officers.

The information operations officer attends and should be a voting member at the Joint Targeting Coordination Board (JTCB) meetings to further coordinate and deconflict information operations with other operations. He must be able to articulate the significance of nonlethal information operations targets relative to the Commander's objectives and guidance. The application of nonlethal means oftentimes better serves the Commander's objectives. Disrupting or denying use of a port facility may be a better alternative than destroying it especially when long-term consequences are considered.

During target nomination, the information operations officer may recommend which Component Command should attack the target.

*Duties and Responsibilities for Phase Two: Target Development*

During target development the information operations officer has the following duties and responsibilities.

- \* Conduct target analysis, validation, and nomination for nonlethal information operations targets.

- \* Ensure nonlethal information operations intelligence requirements are included on the intelligence collection plan to include measures of success that specify collection means expected to provide the indicators of a certain action or inaction.<sup>42</sup>

- \* Represent information operations matters at the Joint Targeting Coordination Board.

- \* Coordinate and deconflict targets with the Component Commands.

*Evaluation Criteria for Phase Two: Target Development*

The information operation officer's **continuous** involvement and participation at the Joint Targeting Coordination Board meeting can ensure that the Joint Forces **consider using all available lethal and nonlethal attack means**. His participation will also help targeteers to **use the most effective fire support measures** and to **provide adequate support**. This phase is perhaps the most important for the information operations officer because success in the target development phase lays the foundation for future operations.

### Phase Three: Weaponneering

Phase Three presents the greatest challenge to the information operations officer because the majority of supporting material, such as the Joint Munitions Effectiveness Manuals (JMEM), used to conduct weaponneering focuses on lethal weapons.<sup>43</sup>

#### *Procedures for Phase Three: Weaponneering*

The information operations officer at the Joint Air Operations Center should participate in the weaponneering phase and be able to articulate the rationale for information operations targets and recommended attack means. While it is difficult to quantify many information operations, the information operations officer should attempt to quantify probable outcomes. Disrupting an enemy's movement along Route Orange from H-12 to H+1 or disabling the enemy's air defense systems in Area Whiskey from H+1 to H+20 illustrate ways to quantify probable outcomes of nonlethal information operations.

#### *Duties and Responsibilities for Phase Three: Weaponneering*

The information operations officer at the Joint Air Operations Center should advise weaponneers on the capabilities, limitations, and employment considerations of nonlethal information operations capabilities and activities. He should also help weaponneers quantify probable outcomes of information operations.

#### *Evaluation Criteria for Phase Three: Weaponneering*

The information operations officer can assist planners to conserve limited capabilities by offering alternatives to lethal strikes. **Considering available lethal and nonlethal attack means** and **providing adequate support** may mean employment of only nonlethal information operations or a combination of lethal and nonlethal means to



achieve the desired effects within a resource-constrained environment. The information operation officer's involvement in the weaponeering phase may **provide for flexibility** especially when responding within a complex, adaptive environment.

#### Phase Four: Force Application

Force application uses the products and information obtained in the first three phases to develop strike packages. The end product of this phase is a recommendation on targets with associated targeting data, delivery means, and assessment criteria. It is in this phase that the information officer can exploit windows of opportunity.

#### *Procedures for Phase Four: Force Application*

The information operations officer at the Joint Air Operations Center should coordinate with both the Combat Plans Division and the Combat Operations Division. He can advise the Plans Division on the capability and availability of nonlethal assets. He should also highlight the Component Commands' requests for nonlethal information operations-specific air missions, such as broadcast, leaflet dissemination, electronic attack. The information operations officer should ensure that the Plans Division annotates all airborne nonlethal assets, such as Commando Solo, on the Air Tasking Order.<sup>44</sup> He should also attempt to influence the planners to support nonlethal information operations requests during their development of the Air Tasking Order and during subsequent execution. The information operations officer must articulate how certain nonlethal information operations meet the Commander's objectives and guidance and target priorities. The information operations officer ensures that information operations targets, effects, and their execution timeline are synchronized on the Air Tasking Order. For example, are planned leaflet drops, EC-130E Commando Solo

broadcasts, and jamming operations synchronized against the same target set for the same time frame and deconflicted to prevent electronic fratricide?

The Operations Division monitors execution of the Air Tasking Order. It may cancel a strike package because previous strikes achieved the desired effects. The information operations officer should take advantage of these opportunities to recommend targets and nonlethal capabilities to resource the cancelled package with other missions.

#### *Duties and Responsibilities for Phase Four: Force Application*

During this phase it is critical that the information operations officer stays abreast of available nonlethal capabilities and activities, potential targets, and the threat picture. With this information he can exploit opportunities, employ nonlethal information operations, and help achieve the Commander's objectives. Even if nonlethal targets are lower on the priority list (i.e., the Joint Integrated Prioritized Target List), the opportunity may arise when only nonlethal information operations may be used. It may not be feasible for aircraft to operate in a certain area given the threat. However, aircraft with a standoff capability, such as an EA-6B Prowler or EC-130E Commando Solo, or platforms capable of disseminating leaflets may be capable of operating safely.

The information operations officer must also continue to advise the targeteers on the capabilities, limitations, and employment considerations of nonlethal information operations capabilities and activities.

#### *Evaluation Criteria for Phase Four: Force Application*

In this phase the information operations officer monitors **airspace coordination**, **provides for flexibility**, and **protects the force**. He ensures that the Air Tasking Order

reflects all airborne information operations dissemination assets operating in the Joint Operations Area. He also monitors the Joint Restricted Frequency List to ensure it reflects all protected frequencies used by information operations. By taking advantage of opportunities, he provides flexibility to the Commander to meet his objectives.

#### Phases Five and Six: Execution Planning and Combat Assessment

Actions in Phase Five include monitoring force application and developing combat assessment criteria. In Phase Six, targeteers, intelligence personnel, and others evaluate the success or failure of operations.

#### *Procedures for Phases Five and Six: Execution Planning and Combat Assessment*

The information operations officer should continue to coordinate with the Combat Operations Division to capitalize on opportunities. He may also develop and recommend assessment criteria for nonlethal information operations scheduled for execution. Unlike lethal operations, there are no standard effects or measurement criteria for nonlethal operations. The information operations officer should attempt to quantify or qualify expected outcomes.

Many specialties, such as operations, targeting, engineering, and intelligence, conduct combat assessment; most of the personnel involved conduct it based on the effects of lethal fires. Aircraft video, satellite imagery, or other intelligence products can estimate the amount of damage done to a target. However, evaluating the success of a nonlethal information operation is sometimes difficult due to time delays between execution and enemy action, subjective interpretation of the enemy's action or inaction, and the lack of technical means available to assess some information operations. The information operations officer can use the measurement criteria developed in Phase Five

to help individuals evaluate nonlethal information operations. The bottom line question is—Was the target affected as expected? Did the enemy turn off its radars? Did the enemy force surrender or cease resistance?

*Duties and Responsibilities for Phases Five and Six: Execution and Assessment*

The information operations officer should monitor both lethal and nonlethal operations during both phases. He can assess how planned operations were executed and recommend restrikes or reallocation for future operations. By monitoring the success of lethal operations, he may be able to create opportunities for future nonlethal operation (i.e., reallocation of strike packages no longer required due to mission success to new nonlethal missions).

*Evaluation Criteria for Phases Five and Six: Execution and Assessment*

In these phases the information operations officer may **provide for flexibility** especially when planning future operations. His **continuous** participation in the planning and targeting processes will allow him to exploit developing opportunities.

Figure 13 summarizes the procedures and duties and responsibilities of the information operations officer during the joint targeting process.

<b>PROCEDURES</b>
1. Participate in the Battlefield Management Cell and Joint Planning Group to plan future targeting.
2. Recommend information operations objectives to the Joint Planning Group.
3. Participate in Air Tasking Order development and weaponeering at the Joint Air Operations Center.
4. Participate in the weaponeering phase of the joint targeting process.
5. Coordinate with both the Combat Plans Division and the Combat Operations Division at the Joint Air Operations Center.
<b>DUTIES &amp; RESPONSIBILITIES</b>
1. Develop and propose information operations-specific objectives and guidance.
2. Conduct target analysis, validation, and nomination for nonlethal information operations targets.
3. Ensure nonlethal information operations intelligence requirements are included on the intelligence collection plan.
4. Represent information operations matters at the Joint Targeting Coordination Board.
5. Coordinate and deconflict targets with the Component Commands.
6. Advise commanders and staff on the capabilities, limitations, and employment considerations of nonlethal information operations capabilities and activities.
7. Help weaponeers quantify probable outcomes of information operations.
8. Develop Priority Intelligence Requirements (PIR) to evaluate the effects of nonlethal information operations targeting.
9. Recommend nonlethal information operations at the Battlefield Management Cell and Joint Planning Group for future targeting.

Figure 13. Procedures and Duties and Responsibilities.

#### **IV: CONCLUSIONS, RECOMMENDATIONS, and IMPLICATIONS**

In no other profession are the penalties for employing untrained personnel so appalling or so irrevocable as in the military.

General Douglas MacArthur<sup>45</sup>

The information operations community needs guidance, doctrine, and tactics, techniques and procedures to synchronize and deconflict its capabilities and activities. Without it, the community will continue to struggle. The preceding chapters and these

recommendations offer solutions for those officers working in this ever-developing field of military operations.

### **Conclusions**

Planners, operators, targeteers, and intelligence professionals need to incorporate nonlethal information operations into the joint targeting process to receive synergistic benefits. There are several areas in which nonlethal information operations can make an impact to assist in achieving this goal.

#### **Personnel and Organization**

Modified tables of organization and equipment (MTOEs) should change now to reflect Officer Personnel Management System (OPMS) XXI functional area 30, information operations. The manning document should reflect branches, functional areas, and additional skill identifiers as required. Additionally, the Information Operations Cell should be of sufficient strength to allow for the full integration of information operations with other operations. Fully-qualified personnel should fill the positions in the Cell. This criteria is especially true for nonlethal specialties, such as psychological operations and public affairs. The psychological operations officer should be trained and educated and ideally have experience with psychological operations. The public affairs officer should be similarly trained, educated, and experienced within his specialty. While filling current positions with personnel who will receive on-the-job training is a short-term fix, in the long-term fully qualified personnel are essential to efficient operations.

The Combined Arms Center, the proponent for U.S. Army information operations, at Fort Leavenworth should recommend resident and non-resident members

of the information operations cell. Public affairs, deception, and psychological operations specialists and other representatives, such as targeters, should represent both the lethal and nonlethal aspects of information operations. Additionally, the Combined Arms Center should develop doctrine and tactics, techniques, and procedures for how an information operations cell conducts staff coordination. While the staff coordination conducted by the information operations officer is similar to other staff officers, such as the fire support officer, doctrine should address the unique aspects of lethal and nonlethal information operations integration. The Combined Arms Center should also recommend organizational changes at the Corps and Division level.

Create a Deputy Chief of Staff for Information Operations (DCS-IO) or establish an information operations directorate under the G/J3 similar to the G3 Operations, Fires, and Plans Directorates. The information operations cell is often subordinated under the Operations or Plans Directorate in the G/J3. Elevating information operations to a higher level would truly make information operations an integrating strategy.

Position at least two information operations officers with nonlethal experience at the Battlefield Coordination Element (BCE) in the Joint Air Operations Center (JAOC). Nonlethal experience is preferable since the majority of personnel in the Battlefield Coordination Element have experience with lethal fires. The officers would co-locate with the Combat Plans and Combat Operations Divisions. Like other members of the Battlefield Coordination Element, the information operations officer would coordinate, deconflict, and synchronize operations with the Air Operations Center.

## Training and Education

The Combined Arms Center should devise a training strategy for future functional area 30 officers and for the Training and Doctrine Command's Centers and Schools. Officers and Noncommissioned Officers should receive training starting with their basic course [i.e., Officer Basic Course (OBC) and Noncommissioned Officer Basic Course (BNCOC)] on the capabilities, limitations, and employment considerations of lethal and nonlethal information operations. As officers and soldiers advance, their professional education should address information operations as an integrating strategy.

Information operations officers should receive training from a variety of Joint and Service schools, such as the Joint Information Warfare Staff Officer Course (JIWSOC), the Psychological Operations Officer Course (POOC), and the Army Deception Planner's Seminar (ADPS). As an interim solution, the Armed Forces Staff College or the Combined Arms Center could post lesson plans of currently available courses. Upon designation as an information operations officer, the officer could enroll in an on-line, self-paced course. The key is to leverage available technology and course material to provide these officers current doctrine and guidance.

All personnel who provide assistance to Corps and Divisions should have some expertise in information operations. Currently, there are numerous military and civilian organizations that provide information operations support. Unfortunately, the majority of the personnel have little to no experience with any information operations capabilities or activities save what they learned on-the-job.<sup>46</sup>



## Doctrine

Common joint and service doctrine and tactics, techniques, and procedures are a weak link. The Combined Arms Center should provide guidance to the field on how to establish an information operations cell prior to and after the full implementation of Functional Area 30. Currently, each Corps organizes its information operations cell differently. Recommending positions with associated branch, functional area, and/or additional skill identifier would provide units a baseline from which to modify.

Doctrine should define and quantify when possible, the effects of information operations. As discussed previously, joint doctrine defines lethal effects and commanders typically quantify those effects. A common framework from which to plan, coordinate, and evaluate nonlethal information operations is needed; clear and concise definitions can provide this framework.

The information operations community in coordination with the Combined Arms Center should modify existing procedures and tools for information operations. What are Target Selection Standards (TSS) for information operations? Can Attack Guidance Matrices or High Value Target and High Payoff Target Lists be modified for information operations? The goal is to minimize new information operations-specific procedures and tools while maximizing the integration of information operations using accepted procedures and tools.

Current U.S. Army doctrine should change to reflect the realities of established Corps-level battle rhythms. Rather than establish a separate Information Operations Working Group (IOWG) meeting, hold the meeting immediately after or in conjunction with the Battlefield Management Cell (BMC)/Joint Planning Group (JPG) meetings. The

majority of the Information Operations Working Group members also attend the Battlefield Management Cell/Joint Planning Group meetings. As any Corps planner will attest the battle rhythm is too full to add another meeting.<sup>47</sup>

### Operations

Like the Component Command representatives, the Joint Task Force information operations officer should be a voting member of the Joint Targeting Coordination Board (JTCB). He is uniquely qualified to articulate the costs and benefits of striking an information operations target. He also has a different perspective than most of the other members since the majority of information operations capabilities and activities are nonlethal. During a campaign, there may be operations or phases, such as pre- and post-combat, which warrant nonlethal information operations as the main effort.

The information operations officer must develop information operations objectives and guidance and evaluation criteria based on realistic (and doctrinal) effects. Due to the iterative nature of the joint targeting process the information operations officer must continually reassess the objectives, guidance, operations, and evaluation criteria to ensure they support each other.

To avoid both electronic and materiel fratricide the Air Tasking Order should include all planned missions and assets that use the airspace in the Joint Operations Area. Typically, the Air Tasking Order has a pejorative connotation to non-Air Force personnel. They often fail to realize that the Order is more a means to coordinate than task. The information operations officer's continuous involvement can ensure the Air Tasking Order reflects nonlethal information operations assets.

## **Implications**

Professionals must avoid becoming mesmerized by technology and its lure of finding a silver bullet. The information operations officer can help commanders leverage technology and integrate a host of lethal and nonlethal capabilities to achieve synergism. He can advise the commander when to use information operations in support of other operations or as the supported operation.

If the joint community fails to develop procedures to integrate nonlethal information operations into the joint targeting process, information operations will continue to be marginalized as a force multiplier, conflict minimizer, and peacetime contributor.

---

## ENDNOTES

<sup>1</sup> Joint Chiefs of Staff, Joint Pub 1, *Joint Warfare of the US Armed Forces* (Washington, DC: National Defense University Press, 11 November 1991), 3.

<sup>2</sup> Joint Chiefs of Staff, Joint Pub 3-0, *Doctrine for Joint Operations* (Washington, DC: Government Printing Office, 1 February 1995), III-25.

<sup>3</sup> Joint Chiefs of Staff, Joint Pub 3-13, *Joint Doctrine for Information Operations* (Washington, DC: Government Printing Office, 9 October 1998), vii.

<sup>4</sup> Department of the Army, TRADOC Pam 525-73, *Military Operations: Concept for Nonlethal Capabilities in Army Operations* (Fort Monroe, VA: Training and Doctrine Command, 1 December 1996), Section II : Terms.

<sup>5</sup> Joint Chiefs of Staff, Joint Pub 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: Government Printing Office, 23 March 1994).

<sup>6</sup> *The Joint Doctrine Encyclopedia* [online edition]; available from <http://www.dtic.mil/doctrine/jrm/ency.htm>, under "TARGETING"; Intellink; accessed 7 October 1998.

<sup>7</sup> Colonel Gerald Cummins, USA, Deputy Commander XVIII Airborne Corps Artillery, telephone interview by author, 27 October 1998.

<sup>8</sup> Modified targeting objective from FM 6-20-10, *Tactics, Techniques, and Procedures for the Targeting Process*, p. 3-14.

<sup>9</sup> Air Land Sea Application (ALSA) Center, FM 90-36, *Multiservice Tactics, Techniques, and Procedures for Targeting* (Washington, DC: Government Printing Office, 25 July 1997), I-3.

<sup>10</sup> FM 90-36, I-4-I-5; and Department of the Air Force, Air Force Pamphlet (AFP) 14-210, *USAF Intelligence Targeting Guide* (Washington, DC: Government Printing Office, 1 February 1998), 9.

<sup>11</sup> FM 90-36, I-6 through I-8.

<sup>12</sup> Joint Pub 3-13, IV-1.

---

<sup>13</sup> This comment is not meant to be derogatory. Currently many officers filling information operations positions do not receive training or education in any of the information operations capabilities or activities, such as psychological operations, deception, and public affairs. One of the recommendations of this monograph is to provide training and education in some, if not all of these areas. There are numerous courses on psychological operations, deception, public affairs, et cetera, which officers could attend prior to assignment as an information operations officer. There is also a Joint Information Warfare Staff and Operations Course (JIWSOC) offered by the Armed Forces Staff College. The U.S. military needs someone with professional training and education not just on-the-job training.

<sup>14</sup> Joint Pub 3-13, IV-4. The JTCB is a group formed by the joint force commander to accomplish broad targeting oversight functions that may include, but is not limited to coordinating targeting information, providing targeting guidance and priorities, and preparing and/or refining joint target lists. The board is normally comprised of representatives from the joint force staff, all components, and if required, component subordinate units. (JP 1-02).

<sup>15</sup> Joint Pub 3-13, IV-3.

<sup>16</sup> All fire support planning principle definitions are found in Joint Publication 3-09, *Doctrine for Joint Fire Support* (Washington, DC: Government Printing Office, 12 May 1998), Chapter III.

<sup>17</sup> Joint Pub 3-13, IV-3.

<sup>18</sup> While this comment seems obvious, many officers mistakenly think the cell *conducts* information operations. It is simply a staff organization that coordinates and deconflicts capabilities and activities. Similarly, a targeting cell does not conduct fire support. Although there are historical examples of information operations cells producing and disseminating leaflets and radio broadcasts, this practice should be avoided. Most cells have neither the expertise nor the capability to conduct independent operations. Uncoordinated products could negatively affect a separate psychological operations campaign or higher-level information operations campaign.

<sup>19</sup> Civil affairs functional area specialties include civil defense; labor; legal; public administration; public education; public finance; public health; public safety; public welfare; civilian supply; economics and commerce; food and agriculture; property control; public communications; public transportation; public works and utilities; arts, monuments, and archives; civil information; cultural affairs; and dislocated civilians.

<sup>20</sup> Armed Forces Staff College (AFSC), AFSC Pub 12, *Joint Information Warfare Staff Officer's Guide* (Norfolk, VA: AFSC, February 1998), 10-13 and Major Michael Warmack, USA, S3, 96<sup>th</sup> Civil Affairs Battalion (Airborne), telephone interview by author, 30 November 1998.

---

<sup>21</sup> 96<sup>th</sup> Civil Affairs Battalion, *Leader's Reference Book* (Ft Bragg, NC: 96<sup>th</sup> Civil Affairs Battalion, 18 September 1997), A-2.

<sup>22</sup> Department of the Army, GTA 41-1-1, *Civil Affairs Information and Planning Guide* (Washington, DC: Government Printing Office, December 1993); and 96<sup>th</sup> Civil Affairs Battalion, *Leader's Reference Book*, A-3.

<sup>23</sup> Joint Pub 1-02, 238.

<sup>24</sup> Department of the Army, FM 90-2, *Military Deception in Army Operations*, Draft (Washington, DC: Government Printing Office, 20 March 1997), iii.

<sup>25</sup> Joint Pub 1-02, 129. For purposes of this monograph, the author limits the electronic attack assets to those that are nonlethal in accordance with its definition.

<sup>26</sup> 111<sup>th</sup> Military Intelligence Brigade, *Military Intelligence Reference Guide* (Fort Huachuca, AZ: USAIS&FH, January 1996), 229; 355<sup>th</sup> Wing Homepage, *The EC-130H "Compass Call,"* URL: <<http://www.dm.af.mil/ech.htm>>, accessed 17 September 1998; Jane's Information Group, *Jane's All the World's Aircraft 1993-94* (UK: Jane's Information Group Limited), 482-483; Jane's Information Group, *Jane's Radar and Electronic Warfare Systems 1998-99* (UK: Jane's Information Group Limited), 389-390, 500, and 504; and *Joint Information Warfare Staff Officer's Guide*.

<sup>27</sup> Joint Pub 1-02, 304.

<sup>28</sup> 4<sup>th</sup> Psychological Operations Group (Airborne), *Capabilities Handbook* (Fort Bragg, NC: Print Company, July 1993); Department of the Army, FM 33-1-1, *Psychological Operations Techniques and Procedures* (Washington, DC: Government Printing Office, 5 May 1994); Psychological Operations Capabilities Briefing prepared by author in May 1998 for Prairie Warrior 98.

<sup>29</sup> Joint Chiefs of Staff, Joint Publication 3-61, *Doctrine for Public Affairs in Joint Operations* (Washington, DC: Government Printing Office, 14 May 1997), GL-3.

<sup>30</sup> Joint Pub 3-61, III-7.

<sup>31</sup> Joint Pub 3-61, III-7.

<sup>32</sup> *Joint Information Warfare Staff Officer's Guide*, 2-12.

<sup>33</sup> Department of the Army, TRADOC Pamphlet 525-73, *Military Operations: Concept for Nonlethal Capabilities in Army Operations* (Fort Monroe, VA: Training and Doctrine Command, 1 December 1996), Appendix B. This chart lists potential nonlethal technologies. Appearance on this list does not necessarily indicate that the Department of

---

Defense is developing these capabilities. Only nonlethal technologies that have an information operations application are included; other nonlethal technologies such as sticky or slicky foams were not included in this chart.

<sup>34</sup> *American Heritage Dictionary of the English Language*, New College Edition, under individual words.

<sup>35</sup> *Joint Information Warfare Staff Officer's Guide*, 16-1.

<sup>36</sup> The JTCB is a group formed by the joint force commander to accomplish broad targeting oversight functions that may include, but is not limited to coordinating targeting information, providing targeting guidance and priorities, and preparing and/or refining joint target lists. The board is normally comprised of representatives from the joint force staff, all components, and if required, component subordinate units. (JP 1-02).

<sup>37</sup> Lieutenant Colonel Alfred Lunt, USA, XVIII Airborne Corps Psychological Operations and Information Operations Officer, email discussions with author, 10 December 1998.

<sup>38</sup> Modified from AFP 14-210, *USAF Intelligence Targeting Guide*, 33-34 and LTC Alfred Lunt.

<sup>39</sup> Target priorities are relative and not absolute; a lower priority target may receive resources prior to a higher priority target for a number of reasons, such as geographical limitations.

<sup>40</sup> LTC Alfred Lunt.

<sup>41</sup> The author recommends that the Joint Task Force send an information operations liaison officer to the Joint Air Operations Center. His duties and responsibilities would mirror those of the Component Command liaison officers.

<sup>42</sup> LTC Alfred Lunt.

<sup>43</sup> The JMEM are a Department of Defense publication series containing data and methodologies for conventional weaponeering.

<sup>44</sup> The ATO is really a synchronization matrix for joint air operations. It is a schedule of all air activity in the Joint Operations Area (JOA). The ATO has three parts: tasking (scheduling) order, special instructions (SPINS), and airspace coordination order (ACO). Colonel Gerald Cummins, USA, Deputy Commander XVIII Airborne Corps Artillery, telephone interview by author, 27 October 1998 and Major Scott Schaeffer, USAF, Joint Multinational Combined Arms Doctrine Directorate, Command and General Staff College, interview by author, 21 September 1998.

---

<sup>45</sup> General Douglas MacArthur, quoted in Robert A. Fitton, *Leadership Quotations from the Military Tradition* (Boulder, CO: Westview Press, 1994), 287.

<sup>46</sup> This comment is based on the author's experience. It is stated only as a basis from which to argue the need for in-house training and education in information operations.

<sup>47</sup> LTC Alfred Lunt.



## BIBLIOGRAPHY

### Articles

- Dodgen, Larry. "Nonlethal Weapons." *U.S. News and World Report*, 4 August 1997, 5.
- Pasternak, Douglas. "Wonder Weapons." *U.S. News and World Report*, 7 July 1997, 38-46.
- Thomas, Timothy L. "The Age of the New Persuaders." *Military Review* (May-June 1997): 72-80.
- \_\_\_\_\_. "Deterring Information Warfare: A New Strategic Challenge." *Parameters* (Winter 1996-97): 81-91.
- \_\_\_\_\_. "Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations." *The Journal of Slavic Military Studies* Vol. 11, No. 1 (March 1998): 40-62.
- \_\_\_\_\_. "The Mind Has No Firewall." *Parameters* (Spring 1998): 84-92.
- (FOUO) Veneklas, Brian. "Nontraditional Targeting Considerations for Joint Information Operations." Article in For Official Use Only (FOUO) *Cyber Sword, The Professional Journal of Joint Information Operations*, Vol. 1, No. 1 (Spring 97): 25-26.

### Books

- Jane's Information Group. *Jane's All the World's Aircraft 1993-94*. UK: Jane's Information Group Limited.
- \_\_\_\_\_. *Jane's Radar and Electronic Warfare Systems 1998-99*. UK: Jane's Information Group Limited.
- Siegel, P.C. *Target Bosnia: Integrating Information Activities in Peace Operations*. Fort McNair: National Defense University Press, 1998.

### Electronic Sources

- U.S. Army Land Information Warfare Activity (LIWA). *LIWA Field Support Team (FST) Compact Disk, Unclassified Edition*. Fort Belvoir, VA: USAINSCOM. 29 SEP 98.
- U.S. Department of Defense. *The Joint Doctrine Encyclopedia* [online edition]; available from <http://www.dtic.mil/doctrine/jrm/ency.htm> on Intellink.

355<sup>th</sup> Wing Homepage. *The EC-130H "Compass Call"*. URL:  
<<http://www.dm.af.mil/ech.htm>>.

### Government Documents

Air Land Sea Application (ALSA) Center. Field Manual (FM) 90-36. *Multiservice Tactics, Techniques, and Procedures for Targeting*. Washington, DC: Government Printing Office, 25 July 1997.

\_\_\_\_\_. FM 90-40. *Nonlethal Weapons-Multiservice Procedures for the Tactical Employment of Nonlethal Weapons*. Washington, DC: Government Printing Office, October 1998.

Armed Forces Staff College (AFSC). AFSC Pub 12. *Joint Information Warfare Staff Officer's Guide*. Norfolk, VA: AFSC, February 1998.

U.S. Army Land Information Warfare Activity (LIWA). *LIWA Targeting Brief for 1<sup>st</sup> Armored Division*. Fort Belvoir, VA: USAINSCOM. 22 April 1998.

U.S. Department of the Air Force. Air Force Pamphlet (AFP) 14-210. *USAF Intelligence Targeting Guide*. Washington, DC: Government Printing Office, 1 February 1998.

U.S. Department of the Army. FM 6-20-10. *Tactics, Techniques, and Procedures for the Targeting Process*. Washington, DC: Government Printing Office, May 1996.

\_\_\_\_\_. FM 6-20-30. *Tactics, Techniques, and Procedures for Fire Support for Corps and Division Operations*. Washington, DC: Government Printing Office, 18 October 1989.

\_\_\_\_\_. FM 6-71. *Tactics, Techniques, and Procedures for Fire Support for the Combined Arms Commander*. Washington, DC: Government Printing Office, 29 September 1994.

\_\_\_\_\_. FM 33-1-1. *Psychological Operations Techniques and Procedures*. Washington, DC: Government Printing Office, 5 May 1994.

\_\_\_\_\_. FM 100-6. *Information Operations*. Washington, DC: Government Printing Office, 27 August 1996.

\_\_\_\_\_. FM 100-15. *Corps Operations*. Washington, DC: Government Printing Office, 29 October 1996.

\_\_\_\_\_. GTA 41-1-1. *Civil Affairs Information and Planning Guide*. Washington, DC: Government Printing Office, December 1993.

- \_\_\_\_\_. Training and Doctrine Command (TRADOC) Pam 525-73, *Military Operations: Concept for Nonlethal Capabilities in Army Operations*. Fort Monroe, VA: Training and Doctrine Command, 1 December 1996.
- U.S. Department of Defense. Joint Pub 1. *Joint Warfare of the US Armed Forces*. Washington, DC: National Defense University Press, 11 November 1991.
- \_\_\_\_\_. Joint Pub 1-02. *Department of Defense Dictionary of Military and Associated Terms*. Washington, DC: Government Printing Office, 23 March 1994.
- \_\_\_\_\_. Joint Pub 3-0. *Doctrine for Joint Operations*. Washington, DC: Government Printing Office, 1 February 1995.
- \_\_\_\_\_. Joint Pub 3-09. *Doctrine for Joint Fire Support*. Washington, DC: Government Printing Office, 12 May 1998.
- \_\_\_\_\_. Joint Pub 3-13. *Joint Doctrine for Information Operations*. Washington, DC: Government Printing Office, 9 October 1998.
- \_\_\_\_\_. Joint Pub 3-13.1. *Joint Doctrine for Command and Control Warfare (C2W)*. Washington, DC: Government Printing Office, 7 February 1996.
- \_\_\_\_\_. Joint Pub 3-60. *Doctrine for Joint Targeting (First Draft)*. Washington, DC: Government Printing Office, 31 July 1997.
- \_\_\_\_\_. Joint Pub 3-61. *Doctrine for Public Affairs in Joint Operations*. Washington, DC: Government Printing Office, 14 May 1997.
- \_\_\_\_\_. Joint Pub 5-0. *Doctrine for Planning Joint Operations*. Washington, DC: Government Printing Office, 13 April 1995.
- \_\_\_\_\_. Joint Pub 5-00.2. *Joint Task Force Planning Guidance and Procedures*. Washington, DC: Government Printing Office, September 1991.
- U.S. Department of the Navy. FMFM 6-18. *Techniques and Procedures for Fire Support Coordination*. Washington, DC: Government Printing Office, 7 March 1992.
- 4<sup>th</sup> Psychological Operations Group (Airborne). *Capabilities Handbook*. Fort Bragg, NC: Print Company, July 1993.
- 96<sup>th</sup> Civil Affairs Battalion. *Leader's Reference Book*. Ft Bragg, NC: 96<sup>th</sup> Civil Affairs Battalion, 18 September 1997.

111<sup>th</sup> Military Intelligence Brigade. *Military Intelligence Reference Guide*. Fort Huachuca, AZ: USAIS&FH, January 1996.

### **Interviews**

Caruso, Mark A. Major, U.S. Army, Plans, Programs, Doctrine, Force Integration and Development, 4<sup>th</sup> Psychological Operations Group (Airborne). Telephone interview by author, 15 December 1998 and email discussions with author, December 1998.

Cummins, Gerald. Colonel, U.S. Army, Deputy Commander XVIII Airborne Corps Artillery. Telephone interview by author, 27 October 1998 and email discussions with author, October through November 1998.

Guerry, Charles. Lieutenant Colonel, U.S. Army, Joint Multinational Combined Arms Doctrine Directorate, U.S. Army Command and General Staff College. Interview by author, 16 September 1998.

Lunt, Alfred. Lieutenant Colonel, U.S. Army, XVIII Airborne Corps Information Operations and Psychological Operations Planner. Email discussions with author, October through December 1998.

Schaeffer, Scott. Major, U.S. Air Force, Joint Multinational Combined Arms Doctrine Directorate, U.S. Army Command and General Staff College. Interview by author, 21 September 1998.

Warmack, Michael. Major, U.S. Army, 96<sup>th</sup> Civil Affairs Battalion (Airborne). Telephone interview by author, 30 November 1998.

### **Monographs and Theses**

Doyle, Kevin J. "Information Operations: A Look at Emerging Army Doctrine and its Operational Implications.: MMAS monograph, School of Advanced Military Studies, Fort Leavenworth, 1995.

Hurst, Elizabeth A. "Shaping the Battlefield with Command and Control Warfare." MMAS thesis, Command and General Staff College, Fort Leavenworth, 1996.

Popovich, Michael J. "The Tactical Employment of Non-Lethal Technologies." MMAS monograph, School of Advanced Military Studies, Fort Leavenworth, 1997.

Woolwine, Stephen M. "C2W: A Battlefield Operating System for Force XXI." MMAS monograph, School of Advanced Military Studies, Fort Leavenworth, 1996.